UNE-EN ISO/IEC 27001. TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. REQUISITOS

La adopción de un sistema de gestión de la seguridad de la información garantiza a todas las organizaciones, en el desarrollo de sus procesos de negocio, la definición de aquellos mecanismos, controles y medidas necesarios para gestionar con la mayor eficiencia la integridad, disponibilidad y confidencialidad de su principal activo, la información.

¿Cuáles son los principales requisitos?

- ✓ **COMPROMISO** y **LIDERAZGO** de la alta dirección en materia de seguridad de la información.
- ✓ Identificación de riesgos por activos y por procesos e implementación de acciones de **CONTROL** sobre los mismos.
- ✓ Adopción de **MEDIDAS ORGANIZATIVAS** de carácter técnico y legal de cara a garantizar la seguridad de la información (mecanismos de acceso físico, lógico, criptográfico, etc.).
- ✓ **GARANTIZAR** la seguridad de la información en el intercambio de la misma con terceros.
- ✓ Redacción de **ACUERDOS** de confidencialidad con empleados y de servicio con proveedores.
- ✓ Disponer de **LICENCIAS** de software utilizados en la organización.
- ✓ Gestión y comunicación de **INCIDENTES** relacionados con la seguridad de la información.
- ✓ Formación y **SENSIBILIZACIÓN** a todo el personal de la organización para garantizar la adecuada gestión de competencias en materia de seguridad de la información.
- ✓ Garantizar la **CONTINUIDAD** de negocio implementando controles/pruebas periódicas en aquellos recursos clave en la seguridad de la información.

¿Qué repercusión tiene en mi organización?

- ✓ Gestión y análisis de riesgos de seguridad de la información.
- ✓ Formalización de contratos de confidencialidad con los empleados y acuerdos de prestación de servicio con proveedores.
- ✓ Controles de acceso a áreas seguras de la empresa.
- ✓ Utilización de sistemas de alimentación ininterrumpida.
- ✓ Uso de licencias legales.
- ✓ Realización de un plan de continuidad de negocio.
- ✓ Realización de pruebas periódicas: fallo en servidor/es, suministro eléctrico, hacking ético, etc.
- ✓ Definición de políticas de seguridad de la información.
- ✓ Gestión y control de usuarios al sistema de la organización.
- ✓ Configuración de firewall, VPN, gestión de copias de seguridad, segmentación de redes, etc.
- ✓ Uso certificado digitales y/o métodos de autenticación de usuario para el intercambio de información.

¿Qué ventajas me aporta?

- ✓ Minimización de la probabilidad de materialización de amenazas (costes de recuperación de la información, pérdida de clientes, interrupción de operaciones, etc.).
- ✓ Rápida respuesta ante eventos que comprometan la continuidad de la organización.
- ✓ Imagen hacia el cliente de implantación de medidas de seguridad acorde con sus exigencias.

¿Qué efectos tiene en el mercado?

- ✓ Imagen de mercado de **EMPRESA SEGURA**.

INTEGRA CONSULTORÍA Y SOSTENIBILIDAD, S.L.

P.I. LA PALMERA

AVDA. LA PALMERA, 49

41.703 DOS HERMANAS. SEVILLA

T: +34 955 451 362